A Finite Presentation of CNOT-dihedral Operators

Matthew Amy, Jianxin Chen, Neil J. Ross

Outline

Quantum circuits

Clifford+T and universal gate sets

CNOT-dihedral gates

Rules for CNOT-dihedral gates

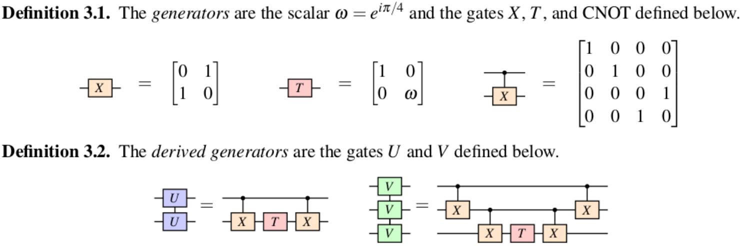
Normal forms

Phase polynomials and uniqueness

Open questions

CNOT-dihedral gates

In the paper, the CNOT-dihedral operators are defined as follows.



Definition 3.1. The *generators* are the scalar $\omega = e^{i\pi/4}$ and the gates X, T, and CNOT defined below.

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad T = \begin{bmatrix} 1 & 0 \\ 0 & \omega \end{bmatrix} \qquad \mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

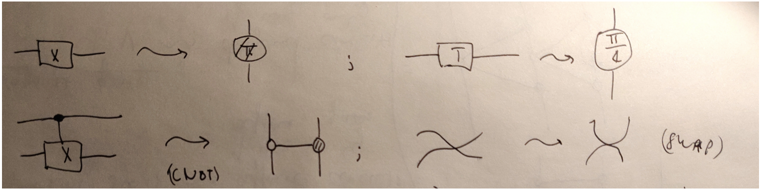
Definition 3.2. The *derived generators* are the gates U and V defined below.

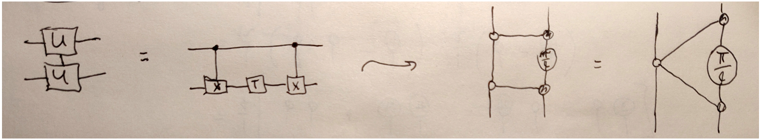
Figure: Amy, Chen and Ross, p. 86.

- The gates X, $CNOT$ and $SWAP$ are called *affine*.
- The gates ω, T, U and V are called *diagonal*.

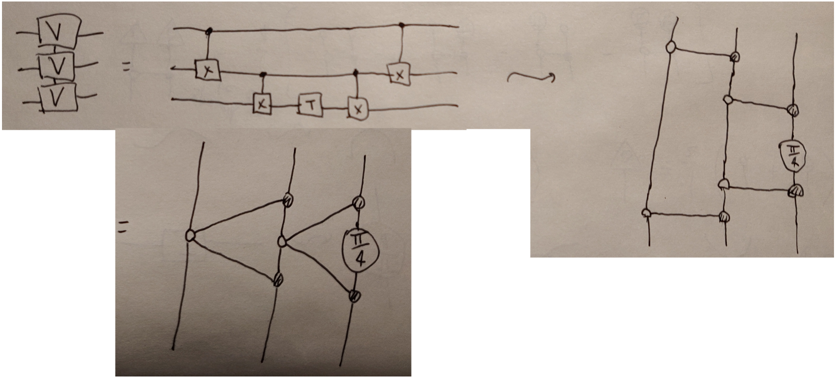
CNOT-dihedral gates in ZX

The gates can be expressed in the ZX-calculus.





CNOT-dihedral gates in ZX



Rules for CNOT-dihedral gates

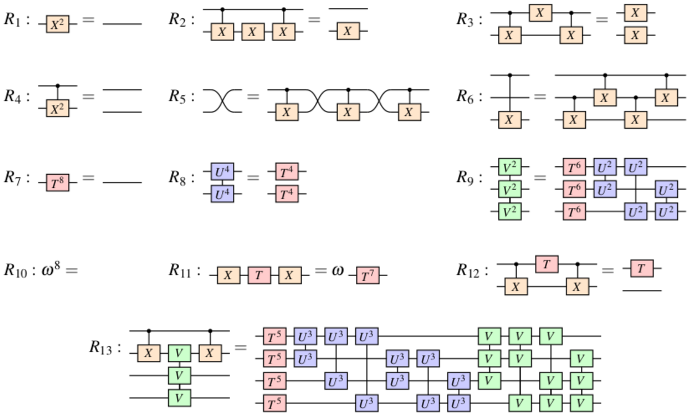
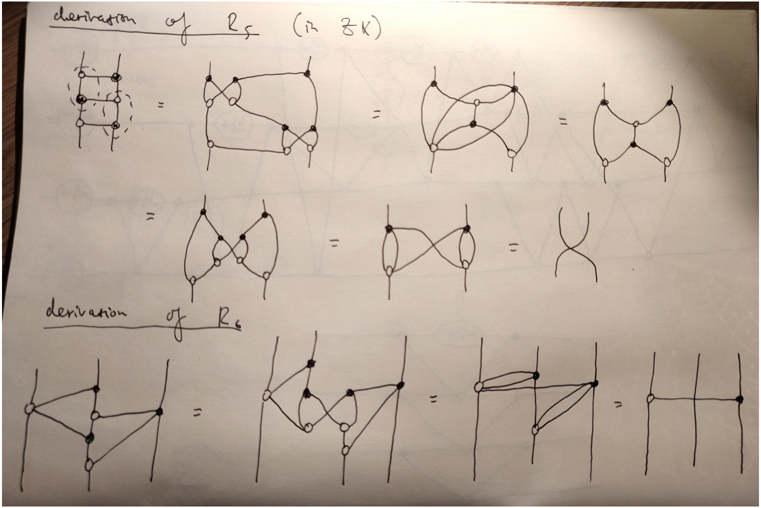


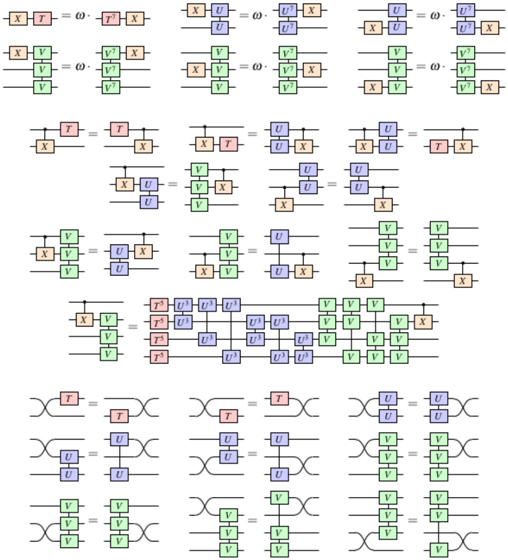
Figure 1: The relations. R_1 through R_6 are affine relations. R_7 through R_{10} are diagonal relations. R_{11} through R_{12} are commutation relations.

Figure: Amy, Chen and Ross, p. 87.

Derivation of R5 and R6 in ZX



Commutation rules



Phase polynomials

Action of a diagonal gate:

$$D|x\rangle = \omega^{p_D(x)}|x\rangle, \quad p_D : \mathbb{Z}_2^n \to \mathbb{Z}_8,$$

$$p_D(x) = \sum_{i=1}^{k} a_i g_i(x).$$

where $a_i \in \mathbb{Z}_8$ and $g_i : \mathbb{Z}_2^n \to \mathbb{Z}_2$ are terms on at most n variables.

$$\omega^k|x\rangle = \omega^k|x\rangle$$

$$T^k|x_1\rangle = \omega^{kx_1}|x_1\rangle$$

$$U^k|x_1x_2\rangle = \omega^{k(x_1\oplus x_2)}|x_1x_2\rangle$$

$$V^k|x_1x_2x_3\rangle = \omega^{k(x_1\oplus x_2\oplus x_3)}|x_1x_2x_3\rangle$$

Therefore for D in normal form we have

$$p_D(x) = a_0 + \sum_i a_i x_i + \sum_{i<j} b_{ij}(x_i \oplus x_j) + \sum_{i<j<k} c_{ijk}(x_i \oplus x_j \oplus x_k)$$

Where $a_i \in \mathbb{Z}_8$, $b_{ij} \in \mathbb{Z}_4$, $c_{ijk} \in \mathbb{Z}_2$ (from the bounds on $deg_X(D)$ for $X = T, U, V$ obtained in normal form).

Uniqueness

Suppose D and D' are distinct diagonal normal forms, then by construction $p_D(x) \neq p_{D'}(x)$ as polynomials. However this does not mean that $\exists y \in \mathbb{Z}_2^n$ s.t. $p_D(y) \neq p_{D'}(y)$.
Counterexample: $4x_1 + 4x_2 + 4(x_1 \oplus x_2) = 0 \bmod 8$ for any $x_1, x_2 \in \mathbb{Z}_2$
To show there exists such a y need a technical lemma: construct a multilinear polynomial $q : \mathbb{Z}_8^n \to \mathbb{Z}_8$ such that $p_D(y) - p_{D'}(y) = q(y)\ \forall y \in \mathbb{Z}_2^n$.
Do this by translating from mod 2 to mod 8:

$$x_i \oplus x_j = x_i + x_j - 2x_i x_j$$

$$x_i \oplus x_j \oplus x_k = x_i + x_j + x_k - 2x_i x_j - 2x_i x_k - 2x_j x_k + 4x_i x_j x_k$$

Then $p_D(x) - p_{D'}(x) \neq 0 \implies q(x) \neq 0$, because of the bounds on a_i, b_{ij} and c_{ijk}. Pick a non-zero term $dx_{i_1} \dots x_{i_k}$ in $q(x)$ then letting y be the vector with 1's in i_jth positions and zero everywhere else we obtain $q(y) = d \neq 0$ and so $D\,|y\rangle \neq D'\,|y\rangle$.

Open questions

- Interaction between ZX and CNOT-dihedral rules (rule 13?)
- The paper doesn't contain an algorithm for normalizing CNOT-dihedral circuits, it uses the properties of the ambient symmetric monoidal structure non-constructively. What could be a rewrite system? Algebraic vs combinatorial description.
- Complexity of CNOT-dihedral circuits.